The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
4/4/2017

SUBJECT:
Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices, including, but not limited to, smartphones, tablets, and watches. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Successful exploitation of the most severe of these vulnerabilities could result in remote code execution in the context of the application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild

SYSTEM AFFECTED:
Android OS builds utilizing Security Patch Levels prior to April 5, 2017

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in the Google Android OS, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Remote code execution vulnerability in Mediaserver (CVE-2017-0538, CVE-2017-0539, CVE-2017-0540, CVE-2017-0541, CVE-2017-0542, CVE-2017-0543)
- Elevation of privilege vulnerability in CameraBase (CVE-2017-0544)
- Elevation of privilege vulnerability in Audioserver (CVE-2017-0545)
- Elevation of privilege vulnerability in SurfaceFlinger (CVE-2017-0546)
- Information disclosure vulnerability in Mediaserver (CVE-2017-0547)
- Denial of service vulnerability in libskia (CVE-2017-0548)
- Denial of service vulnerability in Mediaserver (CVE-2017-0549, CVE-2017-0550, CVE-2017-0551, CVE-2017-0552)
- Elevation of privilege vulnerability in libnl (CVE-2017-0553)
- Elevation of privilege vulnerability in Telephony (CVE-2017-0554)
- Information disclosure vulnerability in Mediaserver (CVE-2017-0555, CVE-2017-0556, CVE-2017-0557, CVE-2017-0558)
- Information disclosure vulnerability in libskia (CVE-2017-0559)
- Information disclosure vulnerability in Factory Reset (CVE-2017-0560)
- Remote code execution vulnerability in Broadcom Wi-Fi firmware (CVE-2017-0561)
- Remote code execution vulnerability in Qualcomm crypto engine driver (CVE-2016-10230)
- Remote code execution vulnerability in kernel networking subsystem (CVE-2016-10229)
- Elevation of privilege vulnerability in MediaTek touchscreen driver (CVE-2017-0562)
- Elevation of privilege vulnerability in HTC touchscreen driver (CVE-2017-0563)
- Elevation of privilege vulnerability in kernel ION subsystem (CVE-2017-0564)
- Vulnerabilities in Qualcomm components (CVE-2016-10237, CVE-2016-10238, CVE-2016-10239)
- Remote code execution vulnerability in v8 (CVE-2016-5129)
- Remote code execution vulnerability in Freetype (CVE-2016-10244)
- Elevation of privilege vulnerability in kernel sound subsystem (CVE-2014-4656)
- Elevation of privilege vulnerability in NVIDIA crypto driver (CVE-2017-0339, CVE-2017-0332, CVE-2017-0327)
- Elevation of privilege vulnerability in MediaTek thermal driver (CVE-2017-0565)
- Elevation of privilege vulnerability in MediaTek camera driver (CVE-2017-0566)
- Elevation of privilege vulnerability in Broadcom Wi-Fi driver (CVE-2017-0567, CVE-2017-0568, CVE-2017-0569, CVE-2017-0570, CVE-2017-0571, CVE-2017-0572, CVE-2017-0573, CVE-2017-0574)
- Elevation of privilege vulnerability in Qualcomm Wi-Fi driver (CVE-2017-0575)
- Elevation of privilege vulnerability in NVIDIA I2C HID driver (CVE-2017-0325)
- Elevation of privilege vulnerability in Qualcomm audio driver (CVE-2017-0454)
- Elevation of privilege vulnerability in Qualcomm crypto engine driver (CVE-2017-0576)
- Elevation of privilege vulnerability in HTC touchscreen driver (CVE-2017-0577)
- Elevation of privilege vulnerability in DTS sound driver (CVE-2017-0578)
- Elevation of privilege vulnerability in Qualcomm sound codec driver (CVE-2016-10231)
- Elevation of privilege vulnerability in Qualcomm video driver (CVE-2017-0579, CVE-2016-10232, CVE-2016-10233)
- Elevation of privilege vulnerability in NVIDIA boot and power management processor driver (CVE-2017-0329)
- Elevation of privilege vulnerability in Synaptics touchscreen driver (CVE-2017-0580, CVE-2017-0581)
- Elevation of privilege vulnerability in Qualcomm Seemp driver (CVE-2017-0462)

- Elevation of privilege vulnerability in Qualcomm Kyro L2 driver (CVE-2017-6423)
- Elevation of privilege vulnerability in kernel file system (CVE-2014-9922)
- Information disclosure vulnerability in kernel memory subsystem (CVE-2014-0206)
- Information disclosure vulnerability in kernel networking subsystem (CVE-2014-3145)
- Information disclosure vulnerability in Qualcomm TrustZone (CVE-2016-5349)
- Information disclosure vulnerability in Qualcomm IPA driver (CVE-2016-10234)
- Denial of service vulnerability in kernel networking subsystem (CVE-2014-2706)
- Denial of service vulnerability in Qualcomm Wi-Fi driver (CVE-2016-10235)
- Elevation of privilege vulnerability in kernel file system (CVE-2016-7097)
- Elevation of privilege vulnerability in Qualcomm Wi-Fi driver (CVE-2017-6424)
- Elevation of privilege vulnerability in Broadcom Wi-Fi driver (CVE-2016-8465)
- Elevation of privilege vulnerability in HTC OEM fastboot command (CVE-2017-0582)
- Elevation of privilege vulnerability in Qualcomm CP access driver (CVE-2017-0583)
- Information disclosure vulnerability in kernel media driver (CVE-2014-1739)
- Information disclosure vulnerability in Qualcomm Wi-Fi driver (CVE-2017-0584)
- Information disclosure vulnerability in Broadcom Wi-Fi driver (CVE-2017-0585)
- Information disclosure vulnerability in Qualcomm Avtimer driver (CVE-2016-5346)
- Information disclosure vulnerability in Qualcomm video driver (CVE-2017-6425)
- Information disclosure vulnerability in Qualcomm USB driver (CVE-2016-10236)
- Information disclosure vulnerability in Qualcomm sound driver (CVE-2017-0586)
- Information disclosure vulnerability in Qualcomm SPMI driver (CVE-2017-6426)
- Information disclosure vulnerability in NVIDIA crypto driver (CVE-2017-0328, CVE-2017-0330)
- Vulnerabilities in Qualcomm components (CVE-2014-9931, CVE-2014-9932, CVE-2014-9933, CVE-2014-9934, CVE-2014-9935, CVE-2014-9936, CVE-2014-9937, CVE-2015-8995, CVE-2015-8996, CVE-2015-8997, CVE-2015-8998, CVE-2015-8999, CVE-2015-9000, CVE-2015-9001, CVE-2015-9002, CVE-2015-9003, CVE-2016-8489)

Successful exploitation of the most severe of these vulnerabilities could result in remote code execution in the context of the application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Remind users to download apps only from trusted vendors in the Play Store.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Google:
https://source.android.com/security/bulletin/2017-04-01.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0206
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1739
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2706
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3145
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4656
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9922
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9931
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9932
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9933
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9934
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9935
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9936
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9937
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8995
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8996
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8997
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8998
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8999
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9000
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9001
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9002
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9003
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10229
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10230
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10231
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10232
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10233
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10234
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10235
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10236
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10237
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10238
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10239
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10244
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5129
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5346
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5349
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7097
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8465
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8489
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0325
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0327
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0328
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0329
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0330
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0332
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0339
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0454
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0462
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0538

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0539
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0540
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0541
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0542
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0543
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0544
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0545
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0546
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0547
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0548
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0549
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0550
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0551
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0552
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0553
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0554
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0555
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0556
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0557
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0558
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0559
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0560
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0561
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0562
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0563
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0564
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0565
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0566
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0567
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0568
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0569
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0570
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0571
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0572
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0573
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0574
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0575
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0576
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0577
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0578
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0579
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0580
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0581
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0582
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0583
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0584
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0585
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0586
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6423
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6424
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6425

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6426